Declassified in Part - Sanitized Copy Approved for Release 2013/02/13: CIA-RDP89B01354R000200270006-5

UNCLASSIFIED

Table 1
Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *	
Access Control and Labels			,		
Discretionary Access Control	A	A ,	. A	Α	- 1
Object Reuse	_		A	Α	- 1
(3) Labels	Α	A .	A	Α	Ì
4 Mandatory Access Control	Α	A	A	Α	
Accountability					
5 Identification & Authentication	Α	A	A	A	
Identification of User Terminal		- A	A	Α	
7 Trusted Path	-	A	A	Α	- 1
8. Audit		A	A	A	
Operational Assurance					
9 System Architecture		A	A	Α	
10 System Integrity	_	A	Ā	A	- 1
11. Trusted Facility Management		Ä	A	A	
12. Trusted Recovery		<u> </u>	A	Ä	
12. Huston Rocovery					-
Life Cycle Assurance					
13. Security Testing		A	A	A	
(14) Design Specification & Verification	_	<u> </u>	A	A	
15. Configuration Management		A	A	A	-
16. Trusted Distribution	_	A	Ą	A	
					ı
Documentation					
17. System Security Statement/Plan	A .	A	A	A	
18. Security Features User's Guide	Α	A	A	A	- 1
19. Trusted Facility Manual	_	A	A	A	- 1
20. Test Documentation	, —	Α	A	A	
21. Design Documentation		_	A	, A	
Environmental Protection					
22. Communications Security (COMSEC)	A	A	A	A	
23. Physical Security	A	A	A	A	
24. TEMPEST		1	A	A	
25. Personnel Security	A	A	A	Ä	
25. Fersonner Security	^		**		
Administrative					
26. Annual Accreditation	A	A	A	A	
27. Dial-up Lines	A T	A	A	A	
28. Protection of Software	A	A	A	A	
29. Access Authentication	A	Α	Α	Α	

Note: "A" means applicable to the identified modes of operation.

5%

^{*} Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

Table 1
Security SAFEGUARDS by Mode of Operation

Access Control and Labels Discretionary Access Control Object Reuse A A A A A A A A A A A A A A A A A A A	SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Object Reuse	Access Control and Labels				
Accountability Accountability (3) Identification & Authentication A A A A A A A A A A A A A A A A A A A	Discretionary Access Control	. A	A	A	Α
Accountability Accountability Soldentification & Authestication A A A A A A A A A A A A A A A A A A A	Object Reuse	_	_	A	A
Accountability (3) Identification & Authentication 6. Identification of User Terminal 7. Trusted Path 8. Audit		Α	Α	A	A
(3) Identification & Authestication A A A A A A A A A A A A A A A A A A A	Mandatory Access Control	A	A	A	A
6 Identification of User Terminal 7 Trusted Path 8 Audit - A A A A A A A A A A A A A A A A A A A	· Accountability				
Trusted Path	5 Identification & Authentication	Α	A	A	A
Operational Assurance 9 System Architecture 10 System Integrity	6. Identification of User Terminal	_	A	A	Α
BAudit Operational Assurance System Architecture System Integrity			* A	A	A
9_System Architecture			A	A	A
System Architecture	Opegational Assurance				
ID System Integrity 11. Trusted Facility Management 12. Trusted Recovery Life Cycle Assurance 13. Security Testing 14. Design Specification & A A A A A A A A A A A A A A A A A A	9 System Architecture	. -	A	A	Α
11. Trusted Facility Management 12. Trusted Recovery Life Cycle Assurance 13. Security Testing 14. Design Specification & Perification Configuration Management 15. Configuration Management 16. Trusted Distribution Documentation 17. System Security Statement/Plan 18. Security Features User's Guide 19. Trusted Facility Manuel 20. Test Documentation 21. Design Documentation 22. Communications Security (COMSEC) 23. Physical Security A A A A A A A A A A A A A A A A A A A		-		A	A
Life Cycle Assurance 13. Security Testing		_	A	A	A
13. Security Testing 14. Design Specification & — — — — — — — — — — — — — — — — — —		· 	-	J	A
13. Security Testing 14. Design Specification &	Life Cycle Assurance			1	
Verification Verification Configuration Management Trusted Distribution Documentation 17. System Security Statement/Plan 18. Security Features User's Guide 19. Trusted Facility Manual 20. Test Documentation			A	A	Α
Configuration Management Trusted Distribution Documentation 17. System Security Statement/Plan 18. Security Features User's Guide A A A A A A A A A A A A A A A A A A A	14 Design Specification &		-	A	A
Documentation 17. System Security Statement/Plan 18. Security Features User's Guide 19. Trusted Facility Manual 20. Test Documentation 21. Design Documentation 22. Communications Security (COMSEC) 23. Physical Security A A A A A A A A A A A A A A A A A A A					
Documentation 17. System Security Statement/Plan 18. Security Features User's Guide 19. Trusted Facility Manuel 20. Test Documentation 21. Design Documentation 22. Communications Security (COMSEC) 23. Physical Security 24. TEMPEST 25. Personnel Security A A A A A A A A A A A A A A A A A A A					I .
17. System Security Statement/Plan 18. Security Features User's Guide 19. Trusted Facility Manuel 20. Test Documentation 21. Design Documentation 22. Communications Security (COMSEC) 23. Physical Security 24. TEMPEST 25. Personnel Security Administrative 26. Annual Accreditation A A A A A A A A A A A A A A A A A A A	(16) Trusted Distribution		^	. ^	^
17. System Security Statement/Plan 18. Security Features User's Guide 19. Trusted Facility Manuel 20. Test Documentation 21. Design Documentation 22. Communications Security (COMSEC) 23. Physical Security 24. TEMPEST 25. Personnel Security Administrative 26. Annual Accreditation A A A A A A A A A A A A A A A A A A A	Documentation	, ,	}		* .
18. Security Features User's Guide 19. Trusted Facility Manual 20. Test Documentation ———————————————————————————————————		A	Α	A	A
20. Test Documentation — A A A A A A A A A A A A A A A A A A		A	A	A	A
20. Test Documentation — A A A A A A A A A A A A A A A A A A			A	A	A
21. Design Documentation — — — — — — — — — — — — — — — — — — —	_		A	Α	A
22. Communications Security (COMSEC) A A A A 23. Physical Security A A A A 24. TEMPEST A A A A 25. Personnel Security A A A A Administrative A A A A Administrative A A A A			_	A	Α .
22. Communications Security (COMSEC) A A A A 23. Physical Security A A A A 24. TEMPEST A A A A 25. Personnel Security A A A A Administrative A A A A Administrative A A A A	Environmental Protection				
23. Physical Security A A A A A A A A A A A A A A A A A A A	22. Communications Security	A	A	A	A
24. TEMPEST A A A A A A A A A A A A A A A A A A A		A	A	A	A
25. Personnel Security A A A A Administrative 26. Annual Accreditation A A A A A		1			1
26. Annual Accreditation A A A A		I .	L	1	•
26. Annual Accreditation A A A A	Administrative				
20. Annual Montalian		A	A	A	A
7 / 1/10 = 11 / 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 /		i .	1	4	
28. Protection of Software A A A A		1	1		1
28. Protection of Software 29. Access Authentication A A A A A A A			1 .		1.

Note: "A" means applicable to the identified modes of operation.

59%

^{*} Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

KAS

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High,	Compartmented	Multilevel *
Access Control and Labels		•		
L Discretionary Access Control	A	' A	A	Α
2 Object Reuse		_	, A	Α
3 Labels	Α	Α	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
3 Identification & Authentication	Α	A	A	A
6. Identification of User Terminal	_	A	A ·	Α
7)Trusted Path	_	A -	A	A
8. Audit		A	A	A
Operational Assurance				
System Architecture		A	A	A
10 System Integrity		A	A	A
11. Trusted Facility Management	. -	A	A	A
12. Trusted Recovery	.—	_	A	A
Life Cycle Assurance				_
13. Security Testing		A	A	A
14) Design Specification & Verification	_	·	A	A .
Configuration Management	_	A	A	A
16. Trusted Distribution	_	A	A	A
Documentation				
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	Ä	A	A	Ą
	.	A	A	A
19. Trusted Facility Manual		Ä	A	A
20. Test Documentation21. Design Documentation	-		Ä	A
Environmental Protection				
22. Communications Security (COMSEC)	Α .	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	Ā	A	A	A
25. Personnel Security	Â	Ä	A	A
25. Personnel Security	^	A	, and the second	"
Administrative	A -	A	A	A
26. Annual Accreditation	A	Â	Ä	Ä
27. Dial-up Lines	A	i	Â	A
28. Protection of Software	A	A	1	1
29 Access Authentication	Α	A A	<u>A</u>	A

Note: "A" means applicable to the identified modes of operation.

(1

^{*} Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

Declassified in Part - Sanitized Copy Approved for Release 2013/02/13 : CIA-RDP89B01354R000200270006-5

UNCLASSIFIED

Table 1
Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel •
Access Control and Labels			_	
Discretionary Access Control	A	A	A	A
Object Reuse			· A	A
(3) Labels	Α	Α	A '	A .
Mandatory Access Control	A	A	A .	, A
Accountability				
5. Identification & Authentication	Α	A	A	A
6. Identification of User Terminal		A	A	A
7.)Trusted Path	_	A	A	A
8 Audit	_	A	A	A
Operational Assurance				
System Architecture		A	A	A
10 System Integrity	-	A	A	A
Ti Trusted Facility Management	_	A	A	A
12. Trusted Recovery	-		A	A
Life Cycle Assurance				
13. Security Testing		A	A	A
(14) Design Specification & Verification	 ·	_	A	A
Configuration Management		, A	A	A
16. Trusted Distribution	· _	Ä	A	A
Documentation				
17. System Security Statement/Plan	A	, A	A	A
18. Security Features User's Guide	Α	A	A	A
19. Trusted Facility Manual	_	A	. A	A
20. Test Documentation	_	Α	A	A
21. Design Documentation	_	-	Α	A
Environmental Protection	i .			
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	Â	A	A	A
25. Personnel Security	Ä	A	Ā	A
Administrative				
26. Annual Accreditation	A	A	A	^ A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	Α .
(29) Access Authentication	A	A	A	A

Note: "A" means applicable to the identified modes of operation.

58%

^{*} Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
.d. Discretionary Access Control	Α	Α	A	. A
(2) Object Reuse			A	A
(a) Labels	Α	A	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
5. Identification & Authentication	Α	A	A	A
6. Identification of User Terminal		A	A .	A
Trusted Path		A	A	A
- 8. Audit		A	A	
Operational Assurance				
System Architecture		A	A	A
10 System Integrity	***	A	A	A
11. Trusted Facility Management		A	A	A
12. Trusted Recovery	-	_	A	A
Life Cycle Assurance				, <u>-</u> , ·
13. Security Testing		A	A	A
14. Design Specification &	· · ·	_	A	A
Verification				
15. Configuration Management	<u></u>	A	A	A
16. Trusted Distribution		A	A	A
Documentation	, -			
17. System Security Statement/Plan	Α	A	A	A
18. Security Features User's Guide	Α	l A	A	A
19. Trusted Facility Manual		A .	A	A
20. Test Documentation		A	A	A
21. Design Documentation		_	A	A
Environmental Protection			-	
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				
26. Annual Accreditation	A	A	Α	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	A	A	A

Note: "A" means applicable to the identified modes of operation.

·

^{*} Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

Declassified in Part - Sanitized Copy Approved for Release 2013/02/13 : CIA-RDP89B01354R000200270006-5

UNCLASSIFIED

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				_
. 1. Discretionary Access Control	A	A	A	Α.
(2)Object Reuse		_	A	A
Labels	A	A	A	A 1
Mandatory Access Control	Α	A	A	A
Accountability				<u> </u>
3 Identification & Authentication	Α	A	A	, A
6 Identification of User Terminal	 .	Α -	A	A
7. Trusted Path		A	A	A
8. Audit	_	A.	A	A
Operational Assurance				
System Architecture	_	A	A	A
10 System Integrity	_	A	A	A
11. Trusted Facility Management	_	A	, A	A
12. Trusted Recovery	_	_	A	A
Life Cycle Assurance			·	
13. Security Testing	_	- A	A	A
(14) Design Specification &		_	A	A
Verification			ŧ	
15. Configuration Management	_	Α	A	A
16. Trusted Distribution		A	A	A
Documentation				
17. System Security Statement/Plan	A	Α	A	A
18. Security Features User's Guide	Α	A	A	A
19. Trusted Facility Manual	-	A	· A	A
20. Test Documentation		A	A	A
21. Design Documentation		_	A	A
Environmental Protection				
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	Α	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				· ·
26. Annual Accreditation	A	A	- A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	A	A	A

Note: "A" means applicable to the identified modes of operation.

10 SSIEIED

^{*} Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

DS 15

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
Discretionary Access Control	Α	A	A	A
2 Object Reuse		_	A	A
3. Labels	A	A	A	A
4. Mandatory Access Control	A	A	A	A
• Accountability				
[5] Identification & Authentication	Α	A	A	A
Adentification of User Terminal		A	· A	A
7. Trusted Path		A	A	A
- 8. Audit	_	A	A	^ A
Operational Assurance				
9 System Architecture		A	A	A
10. System Integrity	· 	A	A	A
. II. Trusted Facility Management		A	A	A
12) Trusted Recovery		_	A	A
Life Cycle Assurance				
13 Security Testing	_	A	A	A
Design Specification & Verification	-		` A	^
15. Configuration Management	_	A	A	A
16. Trusted Distribution	_	A	. A .	A
Documentation			1	
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	A	A	A	A
(19.) Trusted Facility Manual		A	- A	A
20. Test Documentation		A	A	A
21. Design Documentation	_		A	A
Environmental Protection		A	A	A
22. Communications Security (COMSEC)	A			
23. Physical Security	A .	A	A	A .
24. TEMPEST	Α	A	A	A
25. Personnel Security	A	A	Α	A
Administrative				
26. Annual Accreditation	A.	A	A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	Α	A	A

Note: "A" means applicable to the identified modes of operation.

^{*} Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

